

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-341

### Vulnerability Summary for the Week of November 30, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- illustrator	Buffer overflow in Adobe Illustrator CS4 13.0.0 and 14.0.0 allows user-assisted remote attackers to execute arbitrary code via a long DSC Comment in encapsulated Postscript (.eps) file. NOTE: some of these details are obtained from third party information.	2009-12-04	9.3	<a href="#">CVE-2009-4195</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- safari	Stack consumption vulnerability in Apple Safari 4.0.3 on Windows allows remote attackers to cause a denial of service (application crash) via a long URI value (aka url) in the Cascading Style Sheets (CSS) background property.	2009-12-03	9.3	<a href="#">CVE-2009-4186</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a>
bestpractical -- rt	Session fixation vulnerability in html/Elements/SetupSessionCookie in Best Practical Solutions RT 3.0.0 through 3.6.9 and 3.8.x through 3.8.5 allows remote attackers to hijack web sessions by setting the session identifier via a manipulation that leverages a second web server within the same domain.	2009-12-02	7.5	<a href="#">CVE-2009-3585</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
cacti -- cacti	Cacti 0.8.7e and earlier allows remote authenticated administrators to gain privileges by modifying the "Data Input Method" for the "Linux - Get Memory Usage" setting to contain arbitrary commands.	2009-11-30	9.0	<a href="#">CVE-2009-4112</a> <a href="#">BID</a> <a href="#">FULLDISC</a>

ccxvii -- mupdf kowalczyk -- sumatrapdf	Multiple stack-based buffer overflows in pdf_shade4.c in MuPDF before commit 20091125231942, as used in SumatraPDF before 1.0.1, allow remote attackers to cause a denial of service and possibly execute arbitrary code via a /Decode array for certain types of shading that are not properly handled by the (1) pdf_loadtype4shade, (2) pdf_loadtype5shade, (3) pdf_loadtype6shade, and (4) pdf_loadtype7shade functions. NOTE: some of these details are obtained from third party information.	2009-11-30	9.3	CVE-2009-4117 XF VUPEN SECUNIA SECUNIA CONFIRM FULLDISC
ciamos -- ciamos_cms	PHP remote file inclusion vulnerability in modules/pms/index.php in Ciamos CMS 0.9.5 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the module_path parameter.	2009-12-02	7.5	CVE-2009-4156 BID MISC
didier_ernotte -- inforss	infoRSS 1.1.4.2 and earlier extension for Firefox performs certain operations with chrome privileges, which allows remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via the description tag of an RSS feed.	2009-11-29	9.3	CVE-2009-4101 MISC XF VUPEN SECUNIA
eshopbuilder -- eshopbuilde_cms	Multiple SQL injection vulnerabilities in Eshopbuilde CMS allow remote attackers to execute arbitrary SQL commands via the sitebid parameter to (1) home-f.asp and (2) opinions-f.asp; (3) sitebid, (4) id, (5) secText, (6) client-ip, and (7) G_id parameters to more-f.asp; (8) sitebid, (9) id, (10) ma_id, (11) mi_id, (12) secText, (13) client-ip, and (14) G_id parameters to selectintro.asp; (15) sitebid, (16) secText, (17) adv_code, and (18) client-ip parameters to advcount.asp; (19) sitebid, (20) secText, (21) Grp_Code, (22) _method, and (23) client-ip parameters to advview.asp; and (24) sitebid, (25) secText, (26) newsId, and (27) client-ip parameters to dis_new-f.asp.	2009-12-02	7.5	CVE-2009-4155 BUGTRAQ
freebsd -- freebsd	The _rtld function in the Run-Time Link-Editor (rtld) in libexec/rtld-elf/rtld.c in FreeBSD 7.1, 7.2, and 8.0 does not clear the LD_PRELOAD environment variable, which allows local users to gain privileges by executing a setuid or setgid program with a modified LD_PRELOAD variable containing an untrusted search path that points to a Trojan horse library, a different vector than CVE-2009-4147.	2009-12-02	7.2	CVE-2009-4146 BID BUGTRAQ SECUNIA
freebsd -- freebsd	The _rtld function in the Run-Time Link-Editor (rtld) in libexec/rtld-elf/rtld.c in FreeBSD 7.1 and 8.0 does not clear the (1) LD_LIBMAP, (2) LD_LIBRARY_PATH, (3) LD_LIBMAP_DISABLE, (4) LD_DEBUG, and (5) LD_ELF_HINTS_PATH environment variables, which allows local users to gain privileges by executing a setuid or setgid program with a modified variable containing an untrusted search path that points to a Trojan horse library, different vectors than CVE-2009-4146.	2009-12-02	7.2	CVE-2009-4147 SECTRACK BUGTRAQ CONFIRM
g4j.laoneo -- com_gcalendar	SQL injection vulnerability in the Google Calendar GCalendar (com_gcalendar) component 1.1.2, 2.1.4, and possibly earlier versions for Joomla! allows remote attackers to execute arbitrary SQL commands via the gcid parameter. NOTE: some of these details are obtained from third party information.	2009-11-29	7.5	CVE-2009-4099 BID SECUNIA MISC OSVDB
gnu -- grub_2	GNU GRand Unified Bootloader (GRUB) 2.1.97 only compares the submitted portion of a password with the actual password, which makes it easier for physically proximate attackers to conduct brute force attacks and bypass authentication by submitting a password whose	2009-12-01	7.2	CVE-2009-4128 BID

	length is 1.			
hp -- operations_dashboard	HP Operations Dashboard has a default password of j2deployer for the j2deployer account, which allows remote attackers to execute arbitrary code via a session that uses the manager role to conduct unrestricted file upload attacks against the /manager servlet in the Tomcat servlet container. NOTE: this might overlap CVE-2009-3098.	2009-12-03	10.0	CVE-2009-4188 BID MISC
hp -- operations_manager	HP Operations Manager has a default password of OvW*busr1 for the ovwebusr account, which allows remote attackers to execute arbitrary code via a session that uses the manager role to conduct unrestricted file upload attacks against the /manager servlet in the Tomcat servlet container. NOTE: this might overlap CVE-2009-3099 and CVE-2009-3843.	2009-12-03	10.0	CVE-2009-4189 MISC
ibm -- websphere_portal	Unspecified vulnerability in the XMLAccess component in IBM WebSphere Portal 6.1.x before 6.1.0.3 has unknown impact and attack vectors, related to the work directory.	2009-12-02	7.5	CVE-2009-4153 VUPEN CONFIRM
larts -- uploader_activex_control	Multiple stack-based buffer overflows in the Lateral Arts Photobox uploader ActiveX control 1.x before 1.3, and 2.2.0.6, allow remote attackers to execute arbitrary code via a long URL string for the (1) LogURL, (2) ConnectURL, (3) SkinURL, (4) AlbumCreateURL, (5) ErrorURL, or (6) httpsinglehost property value.	2009-12-03	9.3	CVE-2009-1567 VUPEN VUPEN BID BUGTRAQ MISC SECUNIA SECUNIA
linux -- kernel	The mac80211 subsystem in the Linux kernel before 2.6.32-rc8-next-20091201 allows remote attackers to cause a denial of service (panic) via a crafted Delete Block ACK (aka DELBA) packet, related to an erroneous "code shuffling patch."	2009-12-02	7.8	CVE-2009-4026 CONFIRM
linux -- kernel	Race condition in the mac80211 subsystem in the Linux kernel before 2.6.32-rc8-next-20091201 allows remote attackers to cause a denial of service (system crash) via a Delete Block ACK (aka DELBA) packet that triggers a certain state change in the absence of an aggregation session.	2009-12-02	7.1	CVE-2009-4027 CONFIRM CONFIRM
malsmith -- serenity_audio_player	Stack-based buffer overflow in the MplayInputFile function in Serenity Audio Player 3.2.3 and earlier allows remote attackers to execute arbitrary code via a long URL in an M3U file. NOTE: some of these details are obtained from third party information.	2009-11-29	9.3	CVE-2009-4097 SECUNIA MISC OSVDB
mario_matzulla -- calendar_base	SQL injection vulnerability in the Calendar Base (cal) extension before 1.2.1 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-12-02	7.5	CVE-2009-4158 CONFIRM
mauro_lorenzutti -- wfqbe	Unspecified vulnerability in the DB Integration (wfqbe) extension 1.3.1 and earlier for TYPO3 allows local users to execute arbitrary commands via unspecified vectors.	2009-12-02	7.2	CVE-2009-4162 CONFIRM SECUNIA
michal_hadr -- mchtrips	SQL injection vulnerability in the Trips (mchtrips) extension 2.0.0 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-12-02	7.5	CVE-2009-4166 CONFIRM
	Microsoft Internet Explorer 6 and 7 allows remote attackers to execute arbitrary code via vectors involving a call to the getElementsByTagName method for the CSS			

microsoft -- internet_explorer	STYLE tag name, selection of the single element in the returned list, and a change to the outerHTML property of this element, which triggers memory corruption in the Microsoft HTML Viewer (mshtml.dll). NOTE: some of these details are obtained from third party information. NOTE: this issue was originally assigned CVE-2009-4054, but Microsoft assigned a duplicate identifier of CVE-2009-3672. CVE consumers should use this identifier instead of CVE-2009-4054.	2009-12-02	9.3	CVE-2009-3672 MISC BID BUGTRAQ CONFIRM
mozilla -- firefox yoono -- yoono	Yoono extension 6.1.1 for Firefox performs certain operations with chrome privileges, which allows remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via DOM event handlers such as onload.	2009-11-29	9.3	CVE-2009-4100 XF VUPEN BID MISC SECUNIA
mozilla -- firefox sage.mozdev -- sage	Sage 1.4.3 and earlier extension for Firefox performs certain operations with chrome privileges, which allows remote attackers to execute arbitrary commands and perform cross-domain scripting attacks via the description tag of an RSS feed.	2009-11-29	9.3	CVE-2009-4102 XF VUPEN BID MISC SECUNIA MISC
novell -- edirectory	Integer overflow in Novell eDirectory 8.7.3.x before 8.7.3.10 ftf2 and 8.8.x before 8.8.5.2 allows remote attackers to execute arbitrary code via an NDS Verb ox1 request containing a large integer value that triggers a heap-based buffer overflow.	2009-12-03	10.0	CVE-2009-0895 VUPEN CONFIRM
roxio -- creator roxio -- easy_media_creator	Integer overflow in Roxio Easy Media Creator 9.0.136, and Roxio Creator 2010 before SP1, might allow remote attackers to execute arbitrary code via an image with crafted dimensions.	2009-12-03	9.3	CVE-2009-1566 XF VUPEN BID BUGTRAQ MISC SECUNIA
scriptlerim -- radio_isetek_scripti	RADIO istek scripti 2.5 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain user credentials via a direct request for estafresgaftesantusyan.inc.	2009-11-29	7.5	CVE-2009-4096 MISC SECUNIA MISC OSVDB
simple_glossar -- simple_glossar	SQL injection vulnerability in the simple Glossar (simple_glossar) extension 1.0.3 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-12-02	7.5	CVE-2009-4165 CONFIRM
sun -- opensolaris	Unspecified vulnerability in the kernel in Sun OpenSolaris 2009.06 allows remote attackers to cause a denial of service (panic) via unknown vectors, as demonstrated by the vd_solaris2 module in VulnDisco Pack Professional 8.12. NOTE: as of 20091203, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-03	7.8	CVE-2009-4190 MISC MISC
	Unspecified vulnerability in the kernel in Sun Solaris 10 and OpenSolaris 2009.06 on the x86-64 platform allows			

sun -- opensolaris sun -- solaris	local users to gain privileges via unknown vectors, as demonstrated by the vd_sol_local module in VulnDisco Pack Professional 8.12. NOTE: as of 20091203, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	2009-12-03	7.2	CVE-2009-4191 MISC MISC
telepark -- telepark.wiki	Unrestricted file upload vulnerability in ajax/addComment.php in telepark.wiki 2.4.23 and earlier script allows remote attackers to execute arbitrary code by uploading a file with a name containing a NULL byte.	2009-11-29	7.5	CVE-2009-4090 CONFIRM
tw_productfinder -- tw_productfinder	SQL injection vulnerability in the TW Productfinder (tw_productfinder) extension 0.0.2 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-12-02	7.5	CVE-2009-4163 CONFIRM
wikipedia -- wikipedia_toolbar	Unspecified vulnerability in Wikipedia Toolbar extension before 0.5.9.2 for Firefox allows user-assisted remote attackers to execute arbitrary JavaScript with Chrome privileges via vectors involving unspecified Toolbar buttons and the eval function. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-02	9.3	CVE-2009-4127 CONFIRM VUPEN BID SECUNIA

[Back to top](#)

### Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aladdin -- safenet_securewire_access_gateway cisco -- adaptive_security_appliance sonicwall -- e-class_ssl_vp sonicwall -- ssl_vp stonesoft -- stonewgate	Multiple clientless SSL VPN products that run in web browsers, including Stonesoft StoneGate; Cisco ASA; SonicWALL E-Class SSL VPN and SonicWALL SSL VPN; and SafeNet SecureWire Access Gateway, when running in configurations that do not restrict access to the same domain as the VPN, retrieve the content of remote URLs from one domain and rewrite them so they originate from the VPN's domain, which violates the same origin policy and allows remote attackers to conduct cross-site scripting attacks, read cookies that originated from other domains, access the Web VPN session to gain access to internal resources, perform key logging, and conduct other attacks. NOTE: it could be argued that this is a fundamental design problem in any clientless VPN solution, as opposed to a commonly-introduced error that can be fixed in separate implementations. Therefore a single CVE has been assigned for all products that have this design.	2009-12-04	6.8	CVE-2009-2631 CERT-VN XF CONFIRM CONFIRM CONFIRM BID BUGTRAQ FULLDISC
alex_barth -- feed_element_mapper	Cross-site scripting (XSS) vulnerability in Feed Element Mapper module 5.x before 5.x-1.3, 6.x before 6.x-1.3, and 6.x-2.0-alpha before 6.x-2.0-alpha4 for Drupal allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-30	4.3	CVE-2009-4119 BID CONFIRM CONFIRM CONFIRM
an_searchit -- an_searchit	Cross-site scripting (XSS) vulnerability in the [AN] Search it! (an_searchit) extension 2.4.1 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-02	4.3	CVE-2009-4161 BID CONFIRM
	Session fixation vulnerability in html/Elements/SetupSessionCookie in Best Practical			CVE-2009-

bestpractical -- rt	Solutions RT 3.0.0 through 3.6.9 and 3.8.x through 3.8.5 allows remote attackers to hijack web sessions by setting the session identifier via a manipulation that leverages "HTTP access to the RT server," a related issue to CVE-2009-3585.	2009-12-02	6.8	4151 MLIST CONFIRM CONFIRM
cutephp -- cutenews korn19 -- utf-8_cutenews	Static code injection vulnerability in the Categories module in CutePHP CuteNews 1.4.6 and UTF-8 CuteNews before 8b allows remote authenticated users with application administrative privileges to inject arbitrary PHP code into data/category.db.php via the Category Access field.	2009-11-30	6.5	CVE-2009-4113 XF BUGTRAQ MISC
cutephp -- cutenews	Multiple static code injection vulnerabilities in the Categories module in CutePHP CuteNews 1.4.6 allow remote authenticated users with application administrative privileges to inject arbitrary PHP code into data/category.db.php via the (1) category and (2) Icon URL fields; or (3) inject arbitrary PHP code into data/ipban.php via the add_ip parameter.	2009-11-30	6.5	CVE-2009-4115 XF BUGTRAQ MISC
cutephp -- cutenews korn19 -- utf-8_cutenews	Cross-site request forgery (CSRF) vulnerability in CutePHP CuteNews 1.4.6 and UTF-8 CuteNews before 8b allows remote attackers to hijack the authentication of administrators for requests that create new users, including a new administrator, via an adduser action in the editusers module in index.php.	2009-12-02	6.8	CVE-2009-4173 XF BID BUGTRAQ MISC
cutephp -- cutenews korn19 -- utf-8_cutenews	The editnews module in CutePHP CuteNews 1.4.6 and UTF-8 CuteNews before 8b, when magic_quotes_gpc is disabled, allows remote authenticated users with Journalist or Editor access to bypass administrative moderation and edit previously submitted articles via a modified id parameter in a doeditnews action.	2009-12-02	6.0	CVE-2009-4174 XF BID BUGTRAQ MISC
cutephp -- cutenews korn19 -- utf-8_cutenews	CutePHP CuteNews 1.4.6 and UTF-8 CuteNews before 8b allows remote attackers to obtain sensitive information via an invalid date value in the from_date_day parameter to search.php, which reveals the installation path in an error message.	2009-12-02	5.0	CVE-2009-4175 XF BID BUGTRAQ MISC
digium -- asterisk digium -- s800i	rtp.c in Asterisk Open Source 1.2.x before 1.2.37, 1.4.x before 1.4.27.1, 1.6.0.x before 1.6.0.19, and 1.6.1.x before 1.6.1.11; Business Edition B.x.x before B.2.5.13, C.2.x.x before C.2.4.6, and C.3.x.x before C.3.2.3; and s800i 1.3.x before 1.3.0.6 allows remote attackers to cause a denial of service (daemon crash) via an RTP comfort noise payload with a long data length.	2009-12-02	5.0	CVE-2009-4055 CONFIRM XF VUPEN BID BUGTRAQ OSVDB SECTRACK SECUNIA CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
dxm2008 -- xm_easy_personal_ftp_server	XM Easy Personal FTP Server 5.8.0 allows remote authenticated users to cause a denial of service (crash) by uploading or creating a large number of files or directories, then performing a LIST	2009-11-29	4.0	CVE-2009-4108 XF BID BUGTRAQ

	command.			<a href="#">BUGTRAQ SECUNIA</a>
elxis -- elxis_cms	Directory traversal vulnerability in includes/feedcreator.class.php in Elxis CMS allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter.	2009-12-02	5.0	<a href="#">CVE-2009-4154 BID MISC</a>
hp -- nonstop_server hp -- nonstop_server	Unspecified vulnerability in HP NonStop Go6.12.00 through Go6.32.00, Ho6.08.00 through Ho6.18.01, and Jo6.04.00 through Jo6.07.01 allows local users to gain privileges, cause a denial of service, or obtain "access to data" via unknown vectors.	2009-12-02	4.6	<a href="#">CVE-2009-2686 HP HP VUPEN SECUNIA</a>
huawei -- mt882_v100t0o2b020_arg-t	Multiple cross-site scripting (XSS) vulnerabilities in multiple scripts in Forms/ in Huawei MT882 V100R002B020 ARG-T running firmware 3.7.9.98 allow remote attackers to inject arbitrary web script or HTML via the (1) BackButton parameter to error_1; (2) wzConnFlag parameter to fresh_pppoe_1; (3) diag_pppindex_argen and (4) DiagStartFlag parameters to rpDiag_argen_1; (5) wzdmz_active and (6) wzdmzHostIP parameters to rpNATdmz_argen_1; (7) wzVIRTUALSVR_endPort, (8) wzVIRTUALSVR_endPortLocal, (9) wzVIRTUALSVR_IndexFlag, (10) wzVIRTUALSVR_localIP, (11) wzVIRTUALSVR_startPort, and (12) wzVIRTUALSVR_startPortLocal parameters to rpNATvirsvr_argen_1; (13) Connect_DialFlag, (14) Connect_DialHidden, and (15) Connect_Flag parameters to rpStatus_argen_1; (16) Telephone_select, and (17) wzFirstFlag parameters to rpwizard_1; and (18) wzConnectFlag parameter to rpwizPppoe_1.	2009-12-04	4.3	<a href="#">CVE-2009-4196 XF BID MISC</a>
huawei -- mt882_modem_firmware huawei -- mt882_modem	rpwizPppoe.htm in Huawei MT882 V100R002B020 ARG-T running firmware 3.7.9.98 contains a form that does not disable the autocomplete setting for the password parameter, which makes it easier for local users or physically proximate attackers to obtain the password from web browsers that support autocomplete.	2009-12-04	4.7	<a href="#">CVE-2009-4197 XF BID MISC</a>
ibm -- db2 ibm -- db2_universal_database	dasauto in IBM DB2 8 before FP18, 9.1 before FP8, 9.5 before FP4, and 9.7 before FP1 permits execution by unprivileged user accounts, which has unspecified impact and local attack vectors.	2009-12-02	4.6	<a href="#">CVE-2009-4150 CONFIRM CONFIRM</a>
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in the Collaboration component in IBM WebSphere Portal 6.1.x before 6.1.0.3 allows remote attackers to inject arbitrary web script or HTML via the people picker tag.	2009-12-02	4.3	<a href="#">CVE-2009-4152 VUPEN BID CONFIRM SECUNIA</a>
interspire -- knowledge_manager	Directory traversal vulnerability in dialog/file_manager.php in Interspire Knowledge Manager 5 allows remote attackers to read arbitrary files via a .. (dot dot) in the p parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-12-03	5.0	<a href="#">CVE-2009-4192 BID</a>
	Unspecified vulnerability in the Automatic Base Tags			<a href="#">CVE-2009-</a>

it_basetag -- it_basetag	for RealUrl (lt_basetag) extension 1.0.0 for TYPO3 allows remote attackers to conduct "Cache spoofing" attacks via unspecified vectors.	2009-12-02	6.4	<a href="#">4167 BID CONFIRM</a>
joomlatune -- com_proofreader	Multiple cross-site scripting (XSS) vulnerabilities in index.php in the ProofReader (com_proofreader) component 1.0 RC9 and earlier for Joomla! allow remote attackers to inject arbitrary web script or HTML via the URI, which is not properly handled in (1) 404 or (2) error pages.	2009-12-02	4.3	<a href="#">CVE-2009-4157 BID MISC</a>
kaspersky -- kaspersky_anti-virus	kl1.sys in Kaspersky Anti-Virus 2010 9.0.0.463, and possibly other versions before 9.0.0.736, does not properly validate input to IOCTL ox0022coo8, which allows local users to cause a denial of service (system crash) via IOCTL requests using crafted kernel addresses that trigger memory corruption, possibly related to klavemu.kdl.	2009-11-30	4.9	<a href="#">CVE-2009-4114 XF VUPEN SECTRACK BID BUGTRAQ MISC SECUNIA OSVDB</a>
kmint21 -- golden_ftp_server	Directory traversal vulnerability in Golden FTP Server 4.30 Free and Professional, 4.50, and possibly other versions allows remote authenticated users to delete arbitrary files via a .. (dot dot) in the DELE command. NOTE: some of these details are obtained from third party information.	2009-12-03	6.0	<a href="#">CVE-2009-4194 XF MISC SECUNIA MISC</a>
kurt_kunig -- kk_downloader	Unspecified vulnerability in the Simple download-system with counter and categories (kk_downloader) extension 1.2.1 and earlier for TYPO3 allows remote attackers to obtain sensitive information via unknown attack vectors.	2009-12-02	5.0	<a href="#">CVE-2009-4160 CONFIRM</a>
mysql -- mysql	sql/sql_table.cc in MySQL 5.0.x through 5.0.88, 5.1.x through 5.1.41, and 6.0 before 6.0.9-alpha, when the data home directory contains a symlink to a different filesystem, allows remote authenticated users to bypass intended access restrictions by calling CREATE TABLE with a (1) DATA DIRECTORY or (2) INDEX DIRECTORY argument referring to a subdirectory that requires following this symlink.	2009-11-30	6.0	<a href="#">CVE-2008-7247 MLIST MLIST CONFIRM</a>
mysql -- mysql	mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.	2009-11-30	4.0	<a href="#">CVE-2009-4019 MLIST MLIST MLIST CONFIRM CONFIRM CONFIRM CONFIRM</a>
mysql -- mysql	The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.	2009-11-30	6.4	<a href="#">CVE-2009-4028 MLIST MLIST MLIST CONFIRM CONFIRM CONFIRM</a>
	MySQL 5.1.x before 5.1.41 allows local users to bypass			

mysql -- mysql	certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpack_real_data_home value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4098 and CVE-2008-2079.	2009-11-30	4.4	CVE-2009-4030 MLIST MLIST MLIST MLIST CONFIRM CONFIRM
opensolution -- quick.cart	Multiple cross-site request forgery (CSRF) vulnerabilities in Quick.Cart 3.4 allow remote attackers to hijack the authentication of the administrator for requests that (1) delete orders via an orders-delete action to admin.php, and possibly (2) delete products or (3) delete pages via unspecified vectors.	2009-11-30	6.8	CVE-2009-4120 XF BID FULLDISC
opensolution -- quick.cms opensolution -- quick.cms.lite	Multiple cross-site request forgery (CSRF) vulnerabilities in Quick.CMS 2.4 and Quick.CMS.Lite 2.4 allow remote attackers to hijack the authentication of the administrator for requests that (1) delete web pages via a p-delete action to admin.php, and possibly (2) delete products or (3) delete orders via unspecified vectors. NOTE: some of these details are obtained from third party information.	2009-11-30	6.8	CVE-2009-4121 XF BID SECUNIA OSVDB FULLDISC
pear -- pear sendmail -- sendmail	Argument injection vulnerability in Mail/sendmail.php in the Mail package 1.1.14, 1.2.0b2, and possibly other versions for PEAR allows remote attackers to read and write arbitrary files via a crafted \$recipients parameter, and possibly other parameters, a different vulnerability than CVE-2009-4023.	2009-11-29	6.8	CVE-2009-4111 MLIST MLIST MISC
php -- php	The zend_restore_ini_entry_cb function in zend_ini.c in PHP 5.3.0, 5.2.10, and earlier versions allows context-specific attackers to obtain sensitive information (memory contents) and cause a PHP crash by using the ini_set function to declare a variable, then using the ini_restore function to restore the variable.	2009-12-01	6.4	CVE-2009-2626 DEBIAN CONFIRM
roytanck -- wp-cumulus	Cross-site scripting (XSS) vulnerability in tagcloud.swf in the WP-Cumulus Plug-in before 1.23 for WordPress allows remote attackers to inject arbitrary web script or HTML via the tagcloud parameter.	2009-12-02	4.3	CVE-2009-4168 XF VUPEN BID BUGTRAQ CONFIRM MISC SECUNIA
roytanck -- wp-cumulus	Cross-site scripting (XSS) vulnerability in wp-cumulus.php in the WP-Cumulus Plug-in before 1.22 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-02	4.3	CVE-2009-4169 VUPEN BID CONFIRM
	WP-Cumulus Plug-in 1.20 for WordPress, and possibly other versions, allows remote attackers to			CVE-2009-

roytanck -- wp-cumulus	obtain sensitive information via a crafted request to wp-cumulus.php, probably without parameters, which reveals the installation path in an error message.	2009-12-02	5.0	4170 BUGTRAQ MISC
simple_glossar -- simple_glossar	Cross-site scripting (XSS) vulnerability in the simple Glossar (simple_glossar) extension 1.0.3 and earlier for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-02	4.3	CVE-2009-4164 CONFIRM
sun -- java_system_portal_server	Multiple cross-site scripting (XSS) vulnerabilities in the Gateway component in Sun Java System Portal Server 6.3.1, 7.1, and 7.2 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-12-03	4.3	CVE-2009-4187 SUNALERT CONFIRM
telepark -- telepark.wiki	Multiple directory traversal vulnerabilities in telepark.wiki 2.4.23 and earlier allow remote attackers to read arbitrary files via directory traversal sequences in the css parameter to (1) getjs.php and (2) getcsslocal.php; and include and execute arbitrary local files via the (3) group parameter to upload.php.	2009-11-29	6.8	CVE-2009-4088 CONFIRM
yahoo -- messenger	An ActiveX control in YahooBridgeLib.dll for Yahoo! Messenger 9.0.0.2162, and possibly other 9.0 versions, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) by calling the RegisterMe method with a long argument.	2009-12-02	4.3	CVE-2009-4171 XF BID BUGTRAQ

[Back to top](#)

### Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- vpn_client	The StartServiceCtrlDispatcher function in the cvpnd service (cvpnd.exe) in Cisco VPN client for Windows before 5.0.06.0100 does not properly handle an ERROR_FAILED_SERVICE_CONTROLLER_CONNECT error, which allows local users to cause a denial of service (service crash and VPN connection loss) via a manual start of cvpnd.exe while the cvpnd service is running.	2009-11-30	2.1	CVE-2009-4118 VUPEN BID CONFIRM SECUNIA MISC
cutephp -- cutenews	Multiple directory traversal vulnerabilities in CutePHP CuteNews 1.4.6, when magic_quotes_gpc is disabled, allow remote authenticated users with editor or administrative application access to read arbitrary files via a .. (dot dot) in the source parameter in a (1) list or (2) editnews action to the Editnews module, and (3) the save_con[skin] parameter in the Options module. NOTE: vector 3 can be leveraged for code execution by using a .. to include and execute arbitrary local files.	2009-11-30	3.5	CVE-2009-4116 XF XF BUGTRAQ MISC
cutephp -- cutenews korn19 -- utf-8_cutenews	Cross-site scripting (XSS) vulnerability in index.php in CutePHP CuteNews 1.4.6 and UTF-8 CuteNews 8 and 8b, when magic_quotes_gpc is disabled, allows remote attackers to inject arbitrary web script or HTML via the body of a news article in an addnews action.	2009-12-02	2.6	CVE-2009-4172 XF BID BUGTRAQ MISC
ivan_kartolo -- direct_mail	Cross-site scripting (XSS) vulnerability in the newsletter configuration feature in the backend module in the Direct Mail (direct_mail) extension 2.6.4 and earlier for TYPO3 allows remote authenticated users to inject arbitrary web	2009-12-02	3.5	CVE-2009-4159 CONFIRM CONFIRM

	script or HTML via unspecified vectors.			CONFIRM
merkaartor -- merkaartor	Merkaartor 0.14 allows local users to append data to arbitrary files via a symlink attack on the /tmp/merkaartor.log temporary file.	2009-12-03	3.3	CVE-2009-4193 BID
sun -- opensolaris sun -- solaris	Multiple unspecified vulnerabilities in ldap_cachemgr (aka the LDAP client configuration cache daemon) in Sun Solaris 9 and 10, and OpenSolaris before snv_78, allow local users to cause a denial of service (daemon crash) via vectors involving multiple serviceSearchDescriptor attributes and a call to the getldap_lookup function, and unspecified other vectors.	2009-11-29	2.1	CVE-2009-4080 CONFIRM
<a href="#">Back to top</a>				

Last updated December 07, 2009

 Print This Document